Définir un modèle générique de l'ISMS [1] pour PME/PMI

Travail de diplôme réalisé en vue de l'obtention du diplôme d'informaticien de gestion HES

Par :

Alphonse Etienne ETOGA

Conseiller au travail de diplôme :

(Enrico VIGANO, professeur HES)

Genève, le 23 novembre 2006

Haute École de Gestion de Genève (HEG-GE)
Informatique de Gestion

[1] Information Security Management System (Système de Management de la Sécurité de l'Information)

Déclaration

« Ce travail de diplôme est réalisé dans le cadre de l'examen final de la Haute école de gestion de Genève, en vue de l'obtention du titre d'Informaticien de gestion HES. L'étudiant accepte, le cas échéant, la clause de confidentialité. L'utilisation des conclusions et recommandations formulées dans le travail de diplôme, sans préjuger de leur valeur, n'engage ni la responsabilité de l'auteur, ni celle du conseiller au travail de diplôme, du juré et de la HEG. »

« J'atteste avoir réalisé seul le présent travail, sans avoir utilisé des sources autres que celles citées dans la bibliographie. »

Fait à Genève, le 23 novembre 2006

Alphonse Etienne ETOGA

Remerciements

Je tiens à remercier M. Enrico Vigano, mon conseiller, pour sa disponibilité, ses conseils avisés, son soutient durant la réalisation de ce travail. Grâce à son engagement, j'ai participer à l'événement « Mieux comprendre les enjeux et les exigences de la norme ISO/CEI 27001 » organisé par le CLUSIS au cours de laquelle, Ted Humphreys l'un des pères de la norme lui-même nous la présentait.

Je remercie également tous ceux qui de près ou de loin m'ont soutenu durant la réalisation de ce travail.

Sommaire

Le but de ce travail est de définir un modèle générique de l'ISMS pour PME/PMI.

Pour la réalisation de ce travail il était indispensable d'aborder certains sujets permettant de voir l'importance de celui-ci d'une part et d'autre part les éléments indispensables à la réalisation de notre mandat. Nous avons pour cela parlé :

- Des contraintes en matière de sécurité de l'information ;
- de la situation actuelle en matière de sécurité de l'information ;
- de la politique de sécurité ;
- des normes dans le domaine de la sécurité de l'information et,
- finalement du modèle générique de l'ISMS.

Table des matières

Liste des Figures

Introduction

Dans notre environnement d'aujourd'hui, il n'y a pas de jour sans débat sur la sécurité. Au nom de la sécurité les états prennent des décisions allant parfois jusqu'à porter atteinte aux droits humains. Dans cet univers aussi insécurisé, quelle place occupe la sécurité de l'information ?

L'information est un bien qui, comme de nombreux autres biens, ajoute de la valeur à l'organisme[2] et doit par conséquent être protégé. La sécurité de l'information protège l'information des menaces très diverses pour assurer la continuité des activités, réduire au minimum les dommages à l'organisme et maximiser la rentabilité des investissements et les possibilités d'affaires. Un Système de gestion de la sécurité de l'information (SGSI) est une approche systématique pour gérer les informations sensibles d'un organisme et en maintenir la sécurité. Il englobe les personnes, les processus et les systèmes.

Devant cette manne pour les organismes et les risques encourus, la question est de savoir si les organismes se préoccupent vraiment de la sécurité de l'information et si oui assurent-elles une vraie gestion de celle-ci ?

La complexité est l'un des handicapes de la mise en place d'un ISMS dans la plus part des organismes et surtout dans les PME/PMI. Ce travail a donc pour but de proposer un modèle générique de l'ISMS pour PME/PMI.

[2] Agent économique, entité publique (collectivité, administration, ministère, etc.) ou privé (entreprise, société, groupe, firme, etc.).

1. Les contraintes en matière de sécurité

1.1 Les contraintes financières

La sécurité de l'information est aujourd'hui une mission de l'organisme, celle-ci est d'autant plus indispensable que les organismes sont appelées à engager des dépenses parfois assez importantes pour l'assurer, ou pour ne l'avoir pas fait.

Les dirigeants ne pouvant pas investir sans avoir l'idée du ROI (Retour sur Investissement) des fonds dépensés, hésitent souvent à décider pour la mise en place d'un système de management de la sécurité de l'information. Il revient donc au responsable de la sécurité de l'information de faire voir aux instances dirigeantes le bien fondé de la mise en place d'un ISMS.

1.2 Les contraintes juridiques

L'organisme est responsable des dommages subits par elle-même et les tiers pour non respect de la législation en matière de sécurité de l'information. Il est donc indispensable que celle-ci se conforme aux règlements en vigueur dans son secteur d'activité en matière de sécurité de l'information.

1.2.1 L'accord de Bâle II : les risques opérationnels

L'accord de Bâle II, signé en juin 2004, ayant pour objectif de renforcer la stabilité du système bancaire, d'améliorer l'égalité de traitement des banques au niveau mondial en harmonisant les exigences de fonds propre dans les différents pays, est un exemple.

Les risques opérationnels font partie des trois catégories de risques du premier des trois piliers de l'accord de Bâle II.

« Le risque opérationnel se définit comme le risque de pertes résultant de carences ou de défauts attribuables à des procédures, personnels et systèmes internes ou à des événements extérieurs. La définition inclut le risque juridique, mais exclut les risques stratégiques et de réputation.»[3]

[3] Art 644, convergence internationale de la mesure et des normes de fonds propres, Comité de Bâle sur le contrôle bancaire, juin 2004

1.3 Les contraintes vis-à-vis des partenaires de l'organisme

Pour l'image de l'organisme pouvoir garantir la sécurité de son information est un argument à prendre au sérieux. Certains partenaires exigent que leur prestataires soient certifiés ISO pour pouvoir entretenir des relations d'affaires avec eux.

2. La situation actuelle en matière de sécurité de l'information

Aujourd'hui, nous distinguons presque trois cas de figure.

1. les organismes sans politique de sécurité de l'information.
2. les organismes qui ont mis en place une politique de sécurité de l'information mais qui n'assurent pas une gestion de celle-ci.
3. les organismes qui ont une politique de sécurité de l'information et qui ont mis en place un ISMS.

2.1 Les raisons de cet état des choses

Beaucoup sont encore aujourd'hui les organismes qui n'ont pas pris conscience de l'importance de l'information. Pour celles-là, la sécurité de l'information n'est pas du tout une priorité, il suffit parfois tout simplement d'installer un antivirus et le tour est joué. Le contrôle ou la mise à l'abri des mots de passe n'est pas de règle. La mise à jour de l'antivirus n'est pas toujours systématique.

Le deuxième groupe concerne les organismes conscients de la valeur de l'information et qui ont décidé de prendre le taureau par les cornes pour sécuriser ce qui est en quelque sorte le poumon de leur activité. Ces organismes ont mis en place une vraie politique de sécurité de l'information mais, pour des raisons diverses ne disposent pas d'un système de management de celle-ci.

Le troisième groupe englobe toutes les organismes qui non seulement, sont conscientes que quelques artifices technologiques, logiciels et matériels ne suffisent plus à protéger leurs informations critiques mais, que la mise en place d'un système de management de la sécurité de l'information est indispensable pour mettre à l'abri leurs informations.

2.2 La sécurité de l'information une contrainte ou une nécessité

2.2.1 Quelques domaines d'application de la sécurité de l'information

2.2.1.1 Classification et contrôle des ressources

La sécurité de l'information permet l'identification des ressources et la classification de celles-ci en fonction de leur importance. Les propriétaires et les utilisateurs de ces ressources sont clairement définis au cours de la mise en place d'une politique de sécurité de l'information.

2.2.1.2 Ressources humaines

La sensibilisation des utilisateurs aux problèmes sécuritaires est assez importante dans la sécurité de l'information, et en particulier, dans le développement de procédures de sécurité lors des mouvements de personnels (arrivés, mutations et départs)

Le rôle des dirigeants de l'organisme n'est pas à négliger car, la sécurité de l'information est l'une des responsabilités qu'ils doivent assumer et promouvoir.

2.2.1.3 Sécurité physique

La sécurité de l'information doit garantir le traitement physique de l'information ainsi que la sécurisation des locaux et des équipements.

2.2.1.4 Contrôles d'accès

Un système de contrôle d'accès au niveau applicatif, réseau et système ainsi que des problématiques liées à la mobilité et au télétravail doivent être étudiés et mis en place.

2.2.1.5 Plan de continuité

Le contenu d'un plan de continuité incluant la sécurité de l'information est définit.

2.2.1.6 Conformité

Prise en compte des lois, des règles, des standards de l'organisme, et des audits en matière de sécurité de l'information permettant de vérifier la conformité des mesures mises en place.

Au vu de ce qui précède nous constatons l'importance de la sécurité de l'information dans le fonctionnement d'un organisme. Nous pouvons donc sans le moindre doute dire que la sécurité de l'information est une nécessité et de surcroit qu'elle est une obligation si l'organisme veut être en conformité avec les lois, règles et standards en matière de sécurité de l'information.

3. Qu'est-ce qu'une politique de sécurité ?

Une politique de sécurité est un plan d'actions définies pour maintenir un certain niveau de sécurité. Elle reflète la vision stratégique de la direction de l'organisme dans un domaine précis.

Une politique de sécurité a pour objectif de définir :

- Les responsables de la sécurité des domaines qu'elle couvre
- L'organisation des différents acteurs
- Les grandes orientations et les principes génériques à appliquer, techniques et organisationnels

3.1 Les qualités d'une bonne politique de sécurité de l'information

a) être aisément compréhensible
b) être facilement applicable
c) être proactive [4]
d) être courte
e) tenir compte des objectifs business
f) être accessible à tous les collaborateurs
g) être régulièrement mise à jour

3.2 Les points que doit normalement couvrir une politique de sécurité de l'information :

a) Les buts de l´organisme en ce qui concerne la sécurité de l´information
b) Ses principes les plus importants, les standards et les contraintes à respecter
c) La définition des responsabilités (à un niveau générique) pour les principaux aspects de la sécurité de l´information
d) Des références à des documents détaillant les processus, les règlements, les organigrammes, etc.

3.3 Les éléments que doit contenir une politique de sécurité de l'information

a) Confirmation de l'engagement de la direction;
b) La désignation d'une personne responsable de la sécurité de l'information;
c) L'identification de ce qui doit être protégé;
d) L'identification de contre qui et quoi vous devez être protégé;
e) Inclure des considérations de protection de l'information;
f) L'encadrement de l'utilisation des actifs informationnels;
g) Un volet sur la conservation, l'archivage et la destruction de l'information;
h) Un volet sur la propriété intellectuelle;
i) la réponse aux incidents et la préparation d'une enquête, s'il y a lieu;

[4] Qui anticipe les problèmes et prend les mesures pour y faire face de manière positive et provoquer le changement souhaité.

j) L'information des utilisateurs sur l'interdiction des actes illégaux sur les informations et ressources de l'organisme.
k) Comment vérifier son application
l) Où trouver des informations supplémentaires sur les mesures et les processus ?

4. Qu'est-ce qu'un ISMS[5] (Source : Management de la SI – Une approche normative, CLUSIF 2004)

C'est un ensemble d'éléments interactifs permettant à un organisme d'établir une politique et des objectifs en matière de sécurité de l'information, d'appliquer la politique, d'atteindre ces objectifs et de contrôler l'atteinte des objectifs.

La politique de sécurité de l'information donne les grandes orientations de l'organisme en matière de sécurité de l'information et fixe des objectifs quantifiés. Elle est officiellement formulée par la Direction, qui s'engage à fournir les moyens nécessaires pour atteindre ces objectifs.

Elle est cohérente avec les objectifs métiers de l'organisme, et avec les besoins de ses clients et partenaires. Elle est communiquée au sein de l'organisme, sa compréhension par les intervenants externes est vérifiée, elle est revue de façon périodique (en général annuellement) pour rester en adéquation avec les objectifs globaux de l'entité.

L'ISMS est établi, documenté, mis en œuvre et entretenu. Son efficacité est mesurée par rapport aux objectifs de l'organisme, et cette mesure permet d'améliorer en permanence l'ISMS.

L'ISMS est cohérent avec les autres systèmes de management de l'entité, notamment avec le système de management de la qualité, de la sécurité des conditions de travail, et de l'environnement.

L'ISMS inclut donc au minimum :

a) des éléments documentaires (politique, description des objectifs, cartographie des processus impactés, des activités de sécurité, et des mesures),
b) la description de la méthode d'analyse des risques utilisée,
c) les processus impliqués dans la mise en œuvre de la sécurité de l'information,
d) les responsabilités relatives à la sécurité de l'information,
e) les ressources nécessaires à sa mise en œuvre,
f) les activités relatives à la sécurité de l'information,
g) les enregistrements issus des activités relatives à la sécurité de l'information,
h) les (relevés) de mesures prises sur les processus,

[5] Information Security Management System (Système de management de la sécurité de l'information)

i) les actions relatives à l'amélioration de la sécurité de l'information.

L'existence d'un ISMS dans l'organisme permet de renforcer la confiance dans le mode de gestion de la sécurité de l'information.

4.1 Comment mettre en place un ISMS

L'adoption d'un ISMS est une décision stratégique pour un organisme. Sa conception, son implémentation, et son organisation dépendent des besoins de sécurité de l'organisme. Ces besoins sont eux-mêmes fonction du métier de l'organisme, des exigences de sécurité (client/interne) qui en résultent, des processus mis en place, de sa taille et de sa structure.

Pour initialiser une démarche d'ISMS, l'organisme doit :

a) déterminer le périmètre (fonctionnel, géographique, organisationnel, etc.) concerné,
b) identifier parmi les processus de ce périmètre, ceux qui sont concernés par la sécurité de l'information, et leurs risques associés,
c) déterminer les exigences (objectifs, référentiels, méthodes, etc.) nécessaires pour assurer la sécurité des processus,
d) définir les mesures de sécurité nécessaires pour se conformer aux exigences exprimées.

Les processus nécessaires à l'ISMS comprennent ceux relatifs :

a) aux activités de management,
b) à la mise à disposition des ressources,
c) à la réalisation des produits/services
d) aux mesures et à l'amélioration.

Si l'organisme décide d'externaliser un processus ayant une incidence sur la sécurité, il doit en assurer la maîtrise et mentionner dans l'ISMS les moyens de cette maîtrise.

4.2 Pourquoi mettre en place un ISMS

Le Système de Management de la Sécurité de l'information sert à assurer la sécurité dans la durée, à rendre vérifiable de façon formelle cette sécurité et à fournir une confiance aux parties prenantes de l'organisme.

La mise en place d'un ISMS permet donc à l'organisme non seulement d'assurer sa sécurité de l'information à court, moyen et long terme mais de se mettre à l'abri des tracasseries judiciaires en cas de préjudice du à une attaque de son système d'information.

5. La norme BS 7799-2:2002

5.1 Un peu d'histoire (Source : Management de la SI – Une approche normative, CLUSIF 2004)

Au début des années 1990 de grands groupes britanniques (BT, Shell, Marks & Spencer, Nationwide Building Society, etc.) se sont rencontrés au sujet de l'assurance des échanges commerciaux en ligne. L'objectif était alors de proposer un nombre réduits de mesures clés, liées à la sécurité de l'information, que tout entreprise serait à même de mettre en œuvre. Le département des transports et d'industrie britannique (DTI) tenait à ce que ces dix mesures clés soient identifiées et présentées dans une norme de gestion de la sécurité de l'information, il parraine donc la rédaction d'une première version de ce document – dans le respect des normes et standards du BSI (British Standards Institute).

En 1991 un projet de « code de bonnes pratiques » a été réalisé. Il recommandait en particulier la formalisation d'une politique de sécurité de l'information. Cette dernière devait intégrer au minimum huit conditions (au niveau stratégique et opérationnel) ainsi qu'une condition de « conformité » - et être maintenue à jour. Ceci se traduit par l'augmentation du nombre de responsables de la sécurité de l'information chargés de s'assurer de la conformité en accord avec la politique de l'organisme.

En 1995, la BS7799 présente 10 mesures clés intégrant 100 mesures détaillées potentiellement applicables.

En 1998, il adjoint une partie 2 à la BS7799 dans laquelle plus de 100 mesures de sécurité sont détaillées selon le principe du management de la sécurité de l'information (Information Security Management System - ISMS) et fondé sur une approche de maîtrise des risques. La motivation de la partie 2 a été de mettre à disposition les fondements d'un schéma de certification permettant d'attester la conformité à ce qui est devenu la partie 1.

La priorité a été donnée à l'intégration de la problématique d'e-business en les structurant dans la partie 1 de la BS7799, pour que cette norme puisse être présentée à l'ISO. Le nombre de mesures passe alors à 127.

La BS7799-1 :1999 est reconnue après une réflexion au niveau international et devient alors la norme internationale ISO / IEC 17799 en 2000.

La BS7799-2 :2002 remplace la version de 1998 da la BS7799-2 pour mieux s'inspirer des autres systèmes de management déjà existants tels que BS EN ISO 9001 :2000 et BS EN ISO 14001 :1996 afin de permettre une implémentation intégrée des différents systèmes de management.

5.2 Description de la norme (Extrait : Management de la SI – Une approche normative. CLUSIF 2004)

5.2.1 Périmètre de la norme

La norme BS7799-2 :2002 définit des exigences pour planifier, contrôler et améliorer un ISMS. Elle s'applique à tout organisme, mais aussi à toute unité opérationnelle, tout département au sein d'un entreprise ou tout site géographique, dès lors que celui-ci a la responsabilité de son information et donc dispose d'un responsable identifié.

Au sein de l'organisme la norme concerne, aussi bien le système informatique, que les aspects humains et physiques, les processus, etc.

5.2.2 Structure de la norme

La norme est constituée de 2 parties distinctes :

a) le corps du document rappelle et définit les concepts d'ISMS, le modèle « «Plan, Do. Check, Act » (cf. 5.4) et insiste sur les tâches et l'implication du management,
b) les annexes (A, B, C et D) du document

En dehors des chapitres introductifs de toute norme ISO (§1 Champs d'application, §2 Références, §3 Définitions), la norme aborde les thèmes suivants :

a) la notion d'ISMS au travers de l'approche « processus » et du modèle PDCA (§0) ainsi que le parallèle entre l'ISMS et les autres systèmes de management (qualité, environnement) (§0),
b) les jalons et tâches clés de l'ISMS (§4),
c) les implications et les responsabilités du management associés à un ISMS (§5 et 6),
d) l'amélioration continue de l'ISMS (§7).

L'annexe A (normative) établit les objectifs de maîtrise de la sécurité en empruntant les thèmes directeurs de toutes les sections du document ISO 17799. le terme « normatif » signifie que cette annexe est d'application obligatoire pour conformité à la norme BS7799-2.

L'annexe B (informative) présente de manière générique les actions à mettre en œuvre à chaque étape du cycle PDCA.

Enfin les annexes C et D, également informatives, précisent respectivement les similitudes entre les différents systèmes de management (ISO 9001 :2000, ISO 14001 :1996 et BS7799-2 :2002) et les modifications survenues sur les versions antérieures de la norme dans la BS7799-2 :2002.

5.3 *BS7799-2 et ISMS (Extrait : Management de la SI – Une approche normative. CLUSIF 2004)*

La BS7799-2 a été établie pour des managers et leurs équipes afin de fournir un modèle pour mettre en place et gérer un système de management de la Sécurité de l'Information efficace.

La BS7799-2 s'appuie sur une approche processus pour définir, implémenter, mettre en fonction, maîtriser et améliorer l'efficacité de l'organisation d'un ISMS

La démarche du British Standard suit le « Modèle PDCA» (Plan-Do-Check-Act), connu également sous le nom de « Roue de Deming » (cf. ISO9001 :2000) qui s'applique ainsi à tout ISMS. L'approche processus met l'accent sur l'importance des quatre points du modèle PDCA.

La roue de Deming ou modèle PDCA et l'ISMS

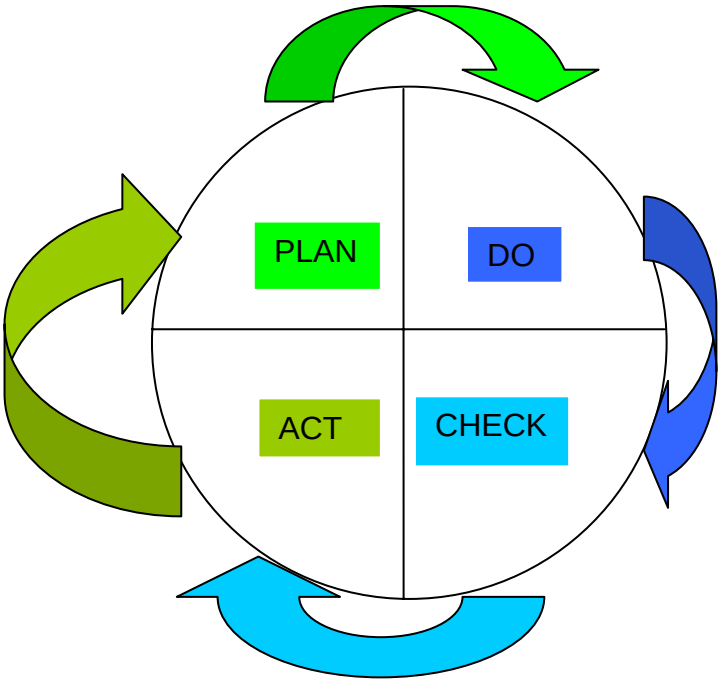

FIG. 1 : ROUE DE DEMING

5.3.1 Planification (Plan)

Consiste à :

a) Délimiter le périmètre de l'ISMS

b) Identifier et évaluer les risques
c) Planifier la gestion des risques identifiés
    - Choisir une méthode de gestion de risque
    - Contrôler la mise en place
    - Traiter le risque (Acceptation, Transfert, Réduction du risque à un niveau acceptable)
d) Documenter
    - SOA : Statement of Applicability (cette documentation identifiera les contrôles choisis pour son environnement et expliquera comment et pourquoi ceux-ci sont appropriés)

5.3.2 Exécution (Do)

Consiste à :

a) Allouer les ressources (Personnes, temps, argent) pour mener à bien l'ISMS
b) Rédiger la documentation
c) Former du personnel concerné par l'ISMS
d) Gérer les risques

Dans la gestion des risques, on aura trois cas de risques possibles :

- Les risques acceptés pour ceux-ci, il n'y aura rien à faire
- Les risques transférés seront assurés par les assurances ou par un partenariat
- Les risques à réduire nécessitent l'implémentation des contrôles identifiés dans la phase de planification, l'assignation des responsabilités pour le contrôle de ces risques et l'identification des risques résiduels.

5.3.3 Vérification (Check)

Consiste à :

a) Des vérifications de routine
b) Apprendre des autres
c) Des audits de l'ISMS (périodiques)

Cette vérification permet de constater l'efficacité des contrôles et que ceux-ci réduisent effectivement les risques pour lesquels ils ont été mis en place.

La vérification permet aussi l'identification de nouveaux risques et les éventuelles inadaptations de la gestion en place.

5.3.4 Action (Act)

Consiste à :

a) Prendre les mesures résultant des constatations faites lors de la phase de vérification
b) Les actions possibles
    - Faire une nouvelle planification (dans le cas ou de nouveaux risques ont été identifiés)

- Engager une phase d'exécution si la phase de vérification montre sa nécessité
- Faire un constat de non-conformité
- Engager des actions correctives ou préventives (elles peuvent être entreprises immédiatement dans certains cas, planifier à long ou moyen terme)

5.4 BS7799-2 et la gestion de la sécurité

Différents acteurs sont concernés par la BS 7799-2 :2002. Ceux-ci trouveront dans la lecture de ce travail les informations sur leurs rôles en fonction des étapes de mise en œuvre d'un ISMS :

a) Analyse des risques,
b) Management du risque,
c) Processus d'amélioration continu.

5.4.1 Qui est concerné par la norme elle-même ?

Toute personne concernée par une démarche d'ISMS et/ou certification est directement concernée par cette norme.

5.4.2 Qui est concerné par l'ISMS ?

a) Propriétaires des informations, Responsables de métiers

Ceux-ci définissent les exigences de sécurité des informations dont ils sont propriétaires. Ils interviennent dans l'étape P du modèle PDCA.

b) Responsable de l'analyse des risques

Il identifie de manière exhaustive les actifs sensibles de l'organisme, les menaces pesant sur ces actifs et les vulnérabilités qu'elles pourraient exploiter. Il intervient dans la phase P/C du modèle PDCA.

c) RSSI

Il propose des mesures de sécurité. Son intervention a lieu dans l'étape P du modèle PDCA.

d) Tous

Mettent en œuvre des mesures de sécurité, participent à l'amélioration de l'ISMS. Cette mise en œuvre se passe dans les étapes D et A du modèle PDCA.

e) Direction Générale

Elle lance la démarche PDCA et valide le traitement du risque. Ces opérations ont lieu dans l'étape P du modèle PDCA

f) Contrôle interne

Audite la démarche, les mesures mises en place. Ceci se passe dans l'étape C du modèle PDCA.

5.4.3 Analyse des risques

Les exigences de sécurité (Disponibilité, Intégrité, Confidentialité) sont définies par les propriétaires des informations.

Le responsable de l'analyse des risques à partir de l'identification exhaustive des actifs sensibles de l'organisme, des menaces pesant sur ces derniers et des vulnérabilités qu'elles pourraient exploiter, évalue les risques.

5.4.4 Gestion du risque

Le RSSI est le principal acteur à qui s'adresse cette partie. Il devra :

a) définir la démarche à suivre (description des étapes nécessaires) pour établir son ISMS,
b) proposer les mesures de sécurité à mettre en place « a priori » (issu de la BS ou non).

La Direction Générale a pour attribution principale :

a) d'affecter les ressources humaines et financières nécessaires à la mise en place des mesures et éventuellement d'accepter certains risques pour l'organisme,
b) de valider et s'engager sur les objectifs de la politique de sécurité.

Les différentes structures de l'organisme devront mettre en place les mesures validées par la Direction Générale.

5.4.5 Processus d'amélioration continue

Le contrôle interne ou Audit a en charge la conduite de missions d'audit interne de la gestion de la politique de sécurité déployée. Cette étape précise les modalités (la périodicité, les objets de la qualité) de ces audits de l'ISMS.

5.5 BS7799-2 et analyse des risques

L'analyse de risques joue un rôle essentiel tout au long de la vie d'un ISMS, aussi bien lors de la définition (le *plan* du modèle PDCA), que lors de la maintenance et de son amélioration (le *check* du PDCA). En effet, la norme stipule qu'une analyse des risques doit être intégrée dans le processus d'établissement de l'ISMS. Idéalement cela peut être réalisé dès la phase de démarrage, afin de lui fournir de la matière première à l'établissement des besoins et des mesures de sécurité à mettre en œuvre. Une approche méthodique est recommandée, toute mesure devant avoir un justificatif formel (écrit et argumenté) à partir des risques identifiés.

Les objectifs de l'ISMS alors fixés en vue de ramener les risques identifiés à un niveau acceptable pour l'organisme.

L'analyse de risques intervient de nouveau en phase de supervision et de révision de l'ISMS (la phase *check*). Cette étape est nécessaire pour garantir la pérennité de l'ISMS et son adéquation face aux évolutions de l'organisme, aux changements d'ordres réglementaires, légaux, et à des nouvelles menaces identifiées. Cette étape, planifiée, est l'occasion d'adapter les procédures qui ont été mise en place dans l'ISMS en fonction des risques, qu'ils soient initiaux ou nouveaux, et de leur niveau d'appréciation.

Aucune méthode d'analyse de risques n'est préconisée dans la BS7799-2. Toute méthode, suffisamment éprouvée, peut être utilisée à condition qu'elle soit bien adaptée à l'ISMS en cours de définition, à l'organisme et contexte d'utilisation (application, type de résultat attendu, spécificité du domaine, compatibilité avec le référentiel de l'entité, etc.).

Les méthodes les plus connues sont EBIOS (DCSSI) et MEHARI (Clusif).

Chacune possède sa propre base de connaissance (Vulnérabilité, méthodes d'attaques, exigences de sécurité, etc.), qui peut ne pas traiter tous les thèmes cités dans la BS7799-2.

6. La norme ISO 17799 (ISO/IEC FDIS 177999)

La norme ISO 17799 est issue de la norme anglaise BS7799. Cette norme constitue un code de bonnes pratiques pour la gestion de la sécurité de l'information. Elle fait l'objet en Grande Bretagne d'un schéma de certification (C : Cure). En effet, ce schéma permet aux entreprises anglaises d'être référencées par rapport à cette norme c'est-à-dire qu'un client qui opère avec cette entreprise a la garantie que ses informations sont gérées de manière plus ou moins sécurisé car un certains nombre de mesures techniques ou non ont été mises en place.

6.1 Description des chapitres de l'ISO 17799 (source : ISO/IEC FDIS 177999)

6.1.1 Politique de sécurité

Ce chapitre mentionne notamment la nécessité pour l'entreprise de disposer d'une politique de sécurité et d'un processus de validation et de révision de cette politique.

6.1.2 Organisation de la sécurité

Ce chapitre comporte trois parties. Une partie traite de la nécessité de disposer au sein d'un organisme d'une organisation dédiée à la mise en place et au contrôle de mesures de sécurité en insistant sur :

a) L'implication de la hiérarchie et sur la coopération qui devrait exister entre les différentes entités de l'organisme,
b) la désignation de propriétaires de l'information, qui seront responsables de leur classification,
c) l'existence d'un processus pour la mise en place de tout nouveau moyen de traitement de l'information.

Une deuxième partie traite des accès aux informations de l'entreprise par une tierce partie. Ces accès doivent être encadrés par un contrat qui stipule les conditions d'accès et les recours en cas de problèmes.

Une troisième partie indique comment traiter du cas où la gestion de la sécurité est externalisée (outsourcing).

6.1.3 Classification des informations

Ce chapitre traite de la nécessité de répertorier l'ensemble des informations (ou types d'information) de l'entreprise et de déterminer leur classification. La mise en place d'une classification de l'information doit s'accompagner de la rédaction de guides pour la définition des procédures de traitement de chaque niveau de classification.

6.1.4 Sécurité du personnel

Ce chapitre mentionne trois types de mesures :

a) Lors du recrutement de personnel, il est tout aussi important d'enquêter sur le niveau de confiance que l'on peut accorder aux personnes qui auront accès à des informations sensibles que de mentionner dans les contrats d'embauche des clauses spécifiques à la sécurité comme une clause de confidentialité.
b) Une sensibilisation à la sécurité doit être proposée à toute personne accédant à des informations sensibles (nouvel arrivant, tierce partie)
c) L'ensemble du personnel doit être informé de l'existence et du mode d'emploi d'un processus de remonté d'incidents.

6.1.5 Sécurité de l'environnement et des biens physiques

Ce chapitre traite de toutes les mesures classiques pour protéger les bâtiments et les équipements :

a) Délimitation de zone de sécurité pour l'accès aux bâtiments (attention aux accès par les livreurs).
b) Mise en place de sécurité physique comme la lutte contre l'incendie ou les dégâts des eaux.
c) Mise en place de locaux de sécurité avec contrôle d'accès et alarmes, notamment pour les salles machines
d) Mise en place de procédures de contrôle pour limiter les vols ou les compromissions
e) Mise en place de procédures pour la gestion de documents dans les bureaux.

6.1.6 Administration

Ce chapitre traite des points suivants :

a) Rédiger et mettre à jour l'ensemble des procédures d'exploitation de l'entreprise (que se soit pour de l'exploitation réseau, système ou sécurité)
b) Rédiger et mettre à jour les critères d'acceptation de tout nouveau système
c) Prévoir un planning pour l'achat de composant ou matériels pour éviter toute interruption de service
d) Mettre en place un certain nombre de politique organisationnelle et technique (anti-virus, messagerie, diffusion de documents électronique en interne ou vers l'extérieur, sauvegarde et restauration, etc.)

6.1.7 Contrôle d'accès

Ce chapitre comprend beaucoup de propositions de mesures par rapport aux autres. Sans être exhaustif on peut cependant retenir :

a) La nécessité pour l'entreprise de disposer d'une politique de contrôle d'accès (qui a droit à quoi et comment il peut y accéder)
b) La mise en place d'une gestion des utilisateurs et de leurs droits d'accès sans oublier la révision de ces droits (gestion des droits, gestion de mots de passe ou plus généralement d'authentifiants)
c) La responsabilité des utilisateurs face à l'accès aux informations (ne pas divulguer son mot de passe, verrouiller son écran quand on est absent par exemple)
d) Des propositions de mesures pour mettre en œuvre la politique de contrôle d'accès comme la compartimentation de réseaux, de firewalls, de proxies, …, la limitation horaire d'accès, un nombre d'accès simultanés limités, etc.
e) La mise en place d'un système de procédures concernant le télétravail.

6.1.8 Développement et maintenance

Ce chapitre, de la même manière que précédemment, propose des mesures incontournables comme des exemples de mise en œuvre. Sans être exhaustif, on peut retenir :

a) La nécessité d'intégrer les besoins de sécurité dans les spécifications fonctionnelles d'un système
b) Des conseils de développement comme la mise en place d'un contrôle systématique des entrées sorties d'un programme.
c) Des propositions d'intégration de services de sécurité comme le chiffrement, la signature électronique, la non-répudiation, ce qui nécessiterait pour l' organisme la définition d'une politique d'usage et de contrôle d'outils à base de cryptographie ainsi qu'une politique de gestion de clés associées
d) La mise en place de procédures pour l'intégration de nouveaux logiciels dans un système déjà opérationnel
e) La mise en place d'une gestion de configuration

6.1.9 Plan de continuité

Ce chapitre traite de la nécessité pour l'organisme de disposer de plans de continuité ainsi que tout le processus de rédaction, de tests réguliers et de mise à jour de ces plans

6.1.10 Conformité et audit de contrôle

Ce chapitre traite pour l'essentiel de deux points :

a) La nécessité pour l'organisme de disposer de l'ensemble des lois et règlements qui s'appliquent aux informations qu'elle manipule et des procédures associées

b) La mise en place de procédures pour le déroulement d'audits de contrôle

On peut donc noter que le contenu de l'ISO 17799 est à la fois un ensemble de mesures techniques et organisationnelles que l'organisme devrait mettre en place pour gérer de manière sécurisée ses informations mais aussi un ensemble de propositions comme l'utilisation de firewall ou la composition de mots de passe (8 caractères, des caractères alphanumériques, …).

Par conséquent il est très intéressant de s'inspirer de cette norme pour s'informer sur les mesures qu'un organisme peut mettre en place pour gérer la sécurité de ses informations. Par contre comme il n'existe pas encore de référence qui permette de situer un organisme sur une échelle de gestion allant d'une mauvaise gestion à la gestion idéale, il est aujourd'hui difficile d'apprécier le respect de cette norme par un organisme.

7. La norme ISO 27001[6] (Source : International Standard ISO/IEC 27001, Première édition 2005-10-15)

L'**ISO 27001** est un Standard international conçu pour fournir un **Information Security Management System (ISMS).**

L'application de l'ISO 27001 garantira aux clients et fournisseurs que la sécurité de l'information est prise au sérieux au sein de l'organisme avec qui ils traitent, parce qu'il aura mis en place des processus à la pointe de la technique pour aborder les menaces et enjeux de la sécurité de l'information.

L'ISO 27001, *Technologies de l'information – Techniques de sécurité – Systèmes de gestion de sécurité de l'information – Exigences,* spécifie les processus qui permettent à un organisme d'établir, de mettre en œuvre, de revoir et de surveiller, de gérer et d'actualiser un ISMS efficace.

7.1 Approche par processus

Grace à son approche par processus cette norme permet :

a) de comprendre les exigences de sécurité de l'information de l'organisme et le besoin d'établissement de politique fixant les objectifs de sécurité pour l'information
b) d'implémenter et opérer des mesures de sécurité pour gérer les risques liés à l'information, en complément de la gestion des risques opérationnels

6 L'ISO/CEI 27001:2005

c) de surveiller et évaluer les performances et l'efficacité de l'ISMS
d) d'assurer une amélioration continue basée sur la mesure des objectifs de sécurité.

Comme pour la norme BS 7799-2 l'approche processus ici met l'accent sur l'importance des quatre points du modèle PDCA.

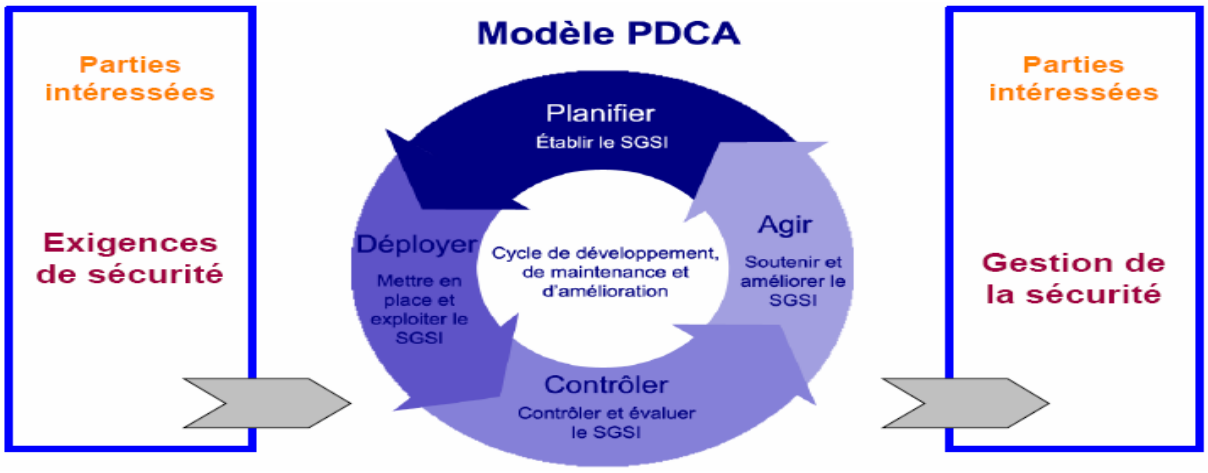

FIG 2 : ROUE DE DEMING POUR ISMS

(SOURCE : OLIVIER LUXEREAU, NETEXPERT SA, 03.10.06)

7.2 ISO 27001 : Compatibilité avec les autres normes

La compatibilité entre la norme ISO 27001 et les autres standards de Systèmes de Gestion (management) tels que :

ISO 9001 :2004 SMQ (Système de Management de la Qualité)

ISO 14001 :2004 SME (Système de Management Environnemental)

Est traitée dans l'annexe « C ».

ISO 27001 est conçu pour permettre à un organisme d'aligner ou d'intégrer son ISMS avec les exigences de ses systèmes de gestion, ce qui est un pas vers la gouvernance de la sécurité de l'information et celle de l'organisme.

7.3 Périmètre de L'ISO 27001

7.3.1 Généralités

Cette norme concerne tout type d'organisme ou d'entité constituante (exemple : Organisme publics, entreprises privées, organisme à but non lucratifs), quelque soient leur taille ou leur activité. Elle spécifie les exigences pour pouvoir **Établir**, **Implémenter**, **Gérer**, **Maintenir** et

Améliorer un **ISMS** documenté en considérant le contexte de l'organisme et de tous ses autres risques « business ».

7.3.2 Application

Les exigences ISO 27001 sont génériques et sont conçues pour être appliquées dans tout type d'organisme indépendamment de la taille ou de la nature.

Les clauses 4, 5, 6, 7 et 8 sont obligatoires pour les organismes qui souhaitent une certification de conformité.

Toute exclusion de mesure de sécurité doit être :

a) fondée par une appréciation des risques
b) justifiée par une acceptation du risque,
c) par une personne désignée
d) qui consolide ses choix par une collecte de preuves

Il est à noter que si un organisme possède déjà un système de gestion de processus « business », il est préférable dans la plupart des cas de satisfaire les exigences de la norme ISO 27001dans le système existant.

7.4 ISO 27001 et Système de Management de la Sécurité de l'Information(ISMS)

7.4.1 Exigences générales

L'organisme devra établir, mettre en œuvre, réviser, surveiller, maintenir et améliorer un ISMS documenté dans le contexte de son « business » et des risques encourus.

7.4.2 Établir et gérer l'ISMS

7.4.2.1 Établir l'ISMS

L'organisme devra :

a) définir la portée et les frontières de son ISMS en fonction des caractéristiques de son « business », de son organisation, de sa localisation de ses actifs et de sa technologie
b) définir la politique de l'ISMS
c) définir l'approche d'évaluation de risque
d) identifier les risques
e) analyser et évaluer les risques
f) identifier et évaluer les options de traitements des risques
g) choisir les objectifs et les actions de traitements des risques
h) obtenir l'approbation de la par de la direction des risques résiduels proposés
i) obtenir l'autorisation de la direction de mettre en œuvre et gérer l'ISMS

j) préparer le SOA[7]

7.4.2.2 Mettre en œuvre et gérer l' ISMS

L'organisme devra :

a) formuler un plan de traitement de risques, qui identifie les actions, les ressources, les responsabilités et les priorités appropriées dans la gestion des risques sur la sécurité de l'information
b) implémenter le plan de traitement de risques dans le but d'atteindre les objectifs identifiés
c) mettre en place les traitements sélectionnés au paragraphe 6.4.2.1
d) définir comment mesurer l'efficacité des traitements sélectionnés et indiquer comment ces mesures doivent être employées pour évaluer l'efficacité des traitements et produire des résultats reproductibles et comparables
e) mettre en place les programmes de formation
f) gérer les différentes opérations de l'ISMS
g) gérer les ressources de l'ISMS
h) mettre en place les procédures permettant la détection rapide des événements en rapport avec la sécurité et, de répondre aux incidents liés à la sécurité

7.4.2.3 Surveiller et réviser l'ISMS

L'organisme devra :

a) Exécuter, surveiller et passer en revue les procédures dans le but :
    - de détecter promptement les erreurs dans les résultats des traitements;
    - d'Identifier promptement les infractions, les brèches de sécurité et les incidents;
    - d'aider les dirigeants à déterminer si les activités de sécurité déléguées ou mises en application par l'informatique se passent comme prévu;
    - d'aider à détecter les événements de sécurité et de ce fait empêcher les incidents de sécurité par l'utilisation des indicateurs; et
    - déterminer si les mesures prises pour résoudre une brèche de sécurité étaient efficaces.
b) Entreprendre l'examen régulier de l'efficacité de l'ISMS, en prenant en considération les résultats des audits de sécurité, les incidents, les suggestions et les feedbacks de toutes les parties prenantes
c) Mesurer l'efficacité des opérations pour s'assurer que les objectifs de sécurité ont été atteints
d) Passer en revue les évaluations des risques à intervalles de temps, les risques résiduels et les niveaux de risques acceptables, en tenant compte des changements :
    - de l'organisme
    - de la technologie

[7] The Statement of Applicability (SOA) est un document qui fournit un résumé des décisions concernant le traitement des risques. Permet de justifier l'exclusion de certains contrôles

- des objectifs et processus business
- des menaces identifiées
- de l'efficacité des opérations mises en place : et
- des événements externes, tels que les changements de loi, d'obligations contractuelles, et du climat social.

e) Conduire des audits internes de l'ISMS à des intervalles planifiés
f) Entreprendre une revue de gestion de l'ISMS de façon régulière pour s'assurer que la portée de celui-ci demeure adéquate et que les améliorations dans ses processus sont identifiées.
g) Mettre à jour le plan de sécurité pour tenir compte des résultats des activités surveillées et révisées.
h) Enregistrer les actions et les événements qui pourraient avoir un impact sur l'efficacité ou la performance de l'ISMS

7.4.2.4 Maintenir et améliorer l'ISMS

L'organisme devra régulièrement:

a) Implémenter les améliorations identifiées de l'ISMS
b) Prendre des mesures préventives et correctives appropriées selon les points 8.2 et 8.3 de la norme. Appliquer les leçons apprises à partir des expériences de sécurité d'autres organismes et de celles de l'organisme lui-même.
c) Communiquer les actions et les améliorations à tous les ayants droits avec un niveau de détails appropriés aux circonstances et, conviendra sur la façon de procéder.
d) S'assurer que les améliorations atteignent les objectifs

7.4.3 Exigences de documentation

7.4.3.1 Généralités

La documentation doit inclure les enregistrements des décisions de gestion, assurer la traçabilité des décisions et politiques de gestion, et assurer que les résultats enregistrés sont reproductibles.

La documentation de l'ISMS inclura :

a) Les rapports documentés de la politique et des objectifs de l'ISMS
b) La portée de l'ISMS
c) Les procédures et commandes à l'appui de l'ISMS
d) La description de la méthode d'évaluation des risques
e) Le rapport d'évaluation des risques
f) Le plan de traitement des risques
g) Les procédures documentées souhaitées par l'organisme pour assurer un planning, les opérations et les activités efficaces de ses processus de sécurité de l'information et décrire comment mesurer l'efficacité des activités
h) Les enregistrements requis par cette norme ; et

i) Le SOA[8]

7.4.3.2 Contrôle des documents

Les documents requis par l'ISMS seront protégés et contrôlés. Une procédure documentée sera établit pour définir les actions de gestion requises pour :

a) approuvez les documents pour l'adéquation avant l'issue ;
b) passer en revue et mettre à jour les documents si nécessaires et les ré-approuver ;
c) s'assurer que les changements et le statut actuel des documents sont identifiés ;
d) s'assurer que les versions appropriées des documents applicables sont disponibles aux points d'utilisation ;
e) s'assurer que les documents demeurent lisibles et aisément identifiables ;
f) s'assurer que les documents sont valables pour ceux qui en ont besoin, et sont transférés, stockés et finalement débarrassés conformément aux procédures applicables à leur classification ;
g) S'assurer que les documents donc l'origine est externe sont identifiés ;
h) s'assurer que la distribution des documents est contrôlée ;
i) empêcher l'utilisation fortuite des documents désuets ; et
j) appliquer leur identification appropriée s'ils sont maintenus pour quelque but que ce soit

7.4.3.3 Contrôle des enregistrements

Les enregistrements seront établis et maintenus pour prouver l'évidence de la conformité aux exigences et l'efficacité des opérations de l'ISMS. Ils seront protégés et contrôlés. L'ISMS prendra en compte les conditions légales ou de normalisation appropriées et les engagements contractuels. Les enregistrements demeureront lisibles, aisément identifiables et recouvrable. Les opérations nécessaires pour l'identification, le stockage, la protection, la récupération, la période de conservation et la disposition des enregistrements seront documentées et mises en application.

[8] Statement of Applicability (Déclaration d'applicabilité)

8. Mise en place d'un modèle générique de l'ISMS pour PME/PMI

La définition de son propre ISMS pour un organisme exige une forte implication de la direction générale. L'organisme est appelé à dégager des ressources humaines et des budgets pour démontrer son ambition de parvenir à intégrer la sécurité de l'information dans son processus d'élaboration de sa stratégie à moyen et long terme. Il serait donc inconcevable que la sécurité de l'information soit l'affaire d'une seule personne.

Le risque ne doit plus de nos jours être vécu comme une fatalité improbable dont il sera toujours possible de réparer les conséquences le jour venu. Les PME / PMI doivent aujourd'hui abandonner le contexte de « pas de temps, pas d'argent » qui leur sert de justificatif de la non mise en place d'une gestion du risque et, mettre en œuvre une politique en matière de sécurité de l'information.

La mise en œuvre d'un système de gestion de la sécurité de l'information dans de nombreux cas est perçue comme une charge sans contrepartie favorable et immédiate pour l'organisme, qui ne dispose pas de critères fiables pour le calcul du facteur de retour sur investissement, pourtant l'intérêt économique des actions visant à assurer la sécuriser des systèmes d'information est de nos jours indéniable.

La mise en œuvre d'un système de gestion de la sécurité de l'information efficace nécessite de replacer les usagers au centre de la réflexion. Il s'agira donc de réaliser un travail très personnalisé, propre à chaque organisme, qui tiendra compte du climat social, des habitudes de travail, de la culture d'entreprise, de la stratégie globale et, bien entendu du secteur d'activité. La politique de sécurité se traduisant notamment par une organisation plus rigoureuse et par la mise en œuvre de procédures pouvant être ressenties parfois comme contraignantes, la forte implication de tous les acteurs est indispensable. Ainsi donc le RSSI (responsable de la sécurité des système d'information) ou toute autre personne désignée pour piloter l'ISMS et pour mener à bien la politique de sécurité de l'information au sein de l'organisme doit savoir qu'elle devra gérer un facteur irrationnel par définition qui est le comportement humain.

L'essentiel, dans cette démarche, est d'identifier parfaitement les risques et d'admettre que l'organisme peut décider d'en assumer certains, sous réserve qu'il apporte la justification économique de ce choix.

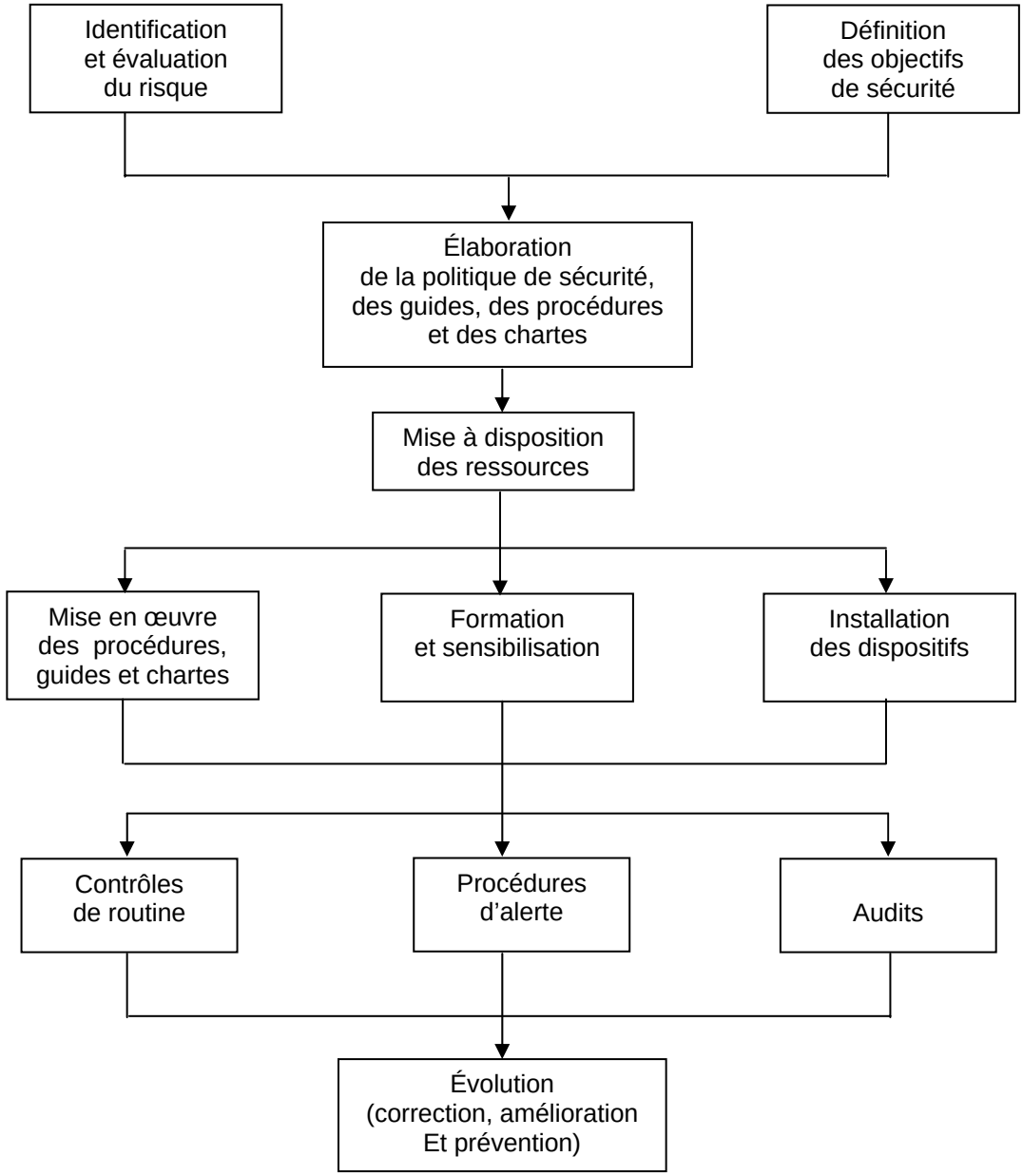

FIG. 3 : MODÈLE GÉNÉRIQUE DE SYSTÈME DE GESTION DE LA SÉCURITÉ DE L'INFORMATION[9]

[9] ***SÉCURITÉ DE L'INFORMATION, ÉLABORATION ET GESTION DE LA POLITIQUE DE L'ENTREPRISE SUIVANT L'ISO 17799, DANIEL LINLAUD,***

8.1 Identification des risques

L'identification des risques pesant sur les éléments du système d'information prend en compte les menaces, les vulnérabilités qui leurs sont associées, et les impacts potentiels en terme de perte de confidentialité, d'intégrité ou de disponibilité.

8.2 Évaluation des risques

La définition d'une approche systématique d'évaluation des risques est importante pour mieux utiliser l'ISMS. L'organisme doit décrire des critères objectifs permettant de mesurer le niveau d'acceptation du risque. L'organisme choisira une méthode d'évaluation des risques parmi les nombreuses qui existent si elle n'a pas sa propre méthode.

8.3 Définition des objectifs

La définition des ses objectifs en matière de sécurité de l'information consiste à évaluer ses propres vulnérabilités puis à analyser les risques en tenant compte de divers paramètres parmi lesquels figurent la criticité des informations concernées, l'impact économique des sinistres potentiels, le risque de leur survenance et le coût des mesures proposées. Il s'agit de réaliser un audit de sécurité qui permettrait la mise en place d'une sécurité efficace après une parfaite identification des risques et des vulnérabilités.

La définition des objectifs de sécurité doit aussi tenir compte des contraintes légales, réglementaires et contractuelles qui s'imposent à l'organisme, ainsi que des principes, objectifs et impératifs propres à son activité.

Les principaux objectifs en matière de politique de sécurité de l'information sont :

- la confidentialité des données ;
- l'intégrité des données ;
- la disponibilité des données ;
- l'irrévocabilité des transactions ;
- l'authenticité des utilisateurs ;
- l'authenticité de l'origine des données ;
- le contrôle des accès.

Les questions suivantes peuvent servir de point de départ à la définition des objectifs en matière de sécurité de l'information.

- Compte tenu de la nature, des objectifs d'affaires et de la mission de l'organisme, quel est le niveau de confidentialité des données requis ?

- Compte tenu de la nature, des objectifs d'affaires et de la mission de l'organisme, quel est le niveau d'intégrité des données requis ?

- Compte tenu de la nature, des objectifs d'affaires et de la mission de l'organisme, quelles sont les attentes de l'organisme en matière de disponibilité des données ?

- Compte tenu de la nature, des objectifs d'affaires et de la mission de l'organisme, quels sont les besoins de l'organisme en matière de non répudiation des données ?

- Compte tenu de la nature, des objectifs d'affaires et de la mission de l'organisme, quels sont les besoins de l'organisme en matière d'authentification des utilisateurs ?

- Compte tenu de la nature, des objectifs d'affaires et de la mission de l'organisme, quels sont les besoins de l'organisme en matière d'authentification de l'origine des données ?

- Compte tenu de la nature, des objectifs d'affaires et de la mission de l'organisme, quels sont les besoins de l'organisme en matière de contrôle d'accès ?

L'identification des réponses à ces questions donnera lieu à un document d'orientation qui devrait identifier les objectifs et les stratégies de l'organisme en matière de sécurité de l'information.

8.4 Élaboration de la politique de sécurité

Les politiques de sécurité de l'information sont en générale des directives de gestion qui établissent les objectifs opérationnels, le cadre de sécurité, les responsabilités et la gouvernance.

L'organisme devrait définir, comme point de départ, une politique qui permet de rencontrer les objectifs en matière de sécurité de l'information élaborés dans le document d'orientation mentionné précédemment (Objectifs). Une fois une première politique cadre en place, l'organisme pourra chercher à élaborer des politiques plus complètes.

La politique de sécurité devrait mettre en évidence la valeur de l'information et la mesure dans laquelle on en a besoin, ainsi que l'importance de la sécurité de l'information pour l'organisme. Elle devrait identifier les exigences minimales au plan de la conformité et des règlements en matière de sécurité. Cette étape inclut des éléments tels la politique de gestion de risques, la classification et l'étiquetage d'information, la sécurité du personnel et du matérielle, les exigences juridiques et contractuelles, l'élaboration et le fonctionnement des systèmes, la planification de la poursuite des activités, la production des rapports sur les

incidents et les exigences d'intervention, l'application des mesures en cas de violation et la sensibilisation à la sécurité de l'information.

La politique peut tenir compte de tout système d'information critique ou des exigences pertinentes. Elle doit cependant identifier les besoins en matière de sécurité de l'information développés en fonction des sept objectifs mentionnés précédemment. Il est nécessaire que soient assignés les rôles et les responsabilités en matière de sécurité de l'information et la distribution des responsabilités dans la structure organisationnelle.

La politique de sécurité de l'information devrait :

- définir les règles et les procédures en matière de sécurité de l'information ;
- définir les procédures pour l'identification de la nature sensible et la classification de l'information ;
- identifier la stratégie de gestion du risque ;
- définir les besoins en matière de continuité des affaires ;
- définir des normes de gestion des ressources humaines ;
- prévoir des plans de sensibilisation des employés et de formation continue en matière de sécurité de l'information ;
- encadrer les obligations légales ;
- identifier les règles de la gestion de l'impartition[10] et des tiers ;
- définir la stratégie de gestion des incidents.

La démarche d'élaboration d'une politique de sécurité est la suivante :

- **Inventaire des actifs informationnels**

Le choix et l'identification de l'actif informationnel à étudier sont critiques au processus d'évaluation des menaces et des risques. Si ces choix sont mal définis, par exemple trop complexe, les résultats de l'évaluation seront difficilement utilisables par l'organisme. Une façon de procéder est d'établir une liste des principaux actifs informationnels, bases de données et systèmes d'information stratégiques dans l'atteinte des objectifs d'affaire de l'organisme.

- **Identification d'un actif informationnel**

En utilisant comme point de départ, l'inventaire des actifs informationnels réalisé précédemment, il s'agira ici de sélectionner un actif informationnel et d'identifier ses principales caractéristiques.

[10] Entente passée entre une entreprise et un tiers pour la gestion continue et l'amélioration des activités reliées à une partie ou à l'ensemble : de fonctions de l'entreprise, d'une infrastructure, de processus opérationnels

- **Identification des vulnérabilités et évaluation des risques qu'elles engendrent**

Une fois l'identification de l'actif informationnel terminée, l'organisme peut commencer l'identification des risques relatifs à ce dernier, c'est-à-dire déterminer les dommages potentiels qu'elle encourt en cas d'atteinte à cet actif informationnel. Au terme de cette étape, on obtient un catalogue des risques qui menacent l'actif étudié.

- **Politique de gestion des risques**

Les risques identifiés doivent être assumés, couverts ou transférés. Le catalogue des risques indiquera obligatoirement le statut de chaque risque, pour permettre l'évaluation du niveau de sécurité. Pour faciliter la détermination du traitement de chaque risque identifié, le catalogue de risques peut être représenté dans un tableau comme celui qui suit. Les sinistres n'ayant pas la même gravité sur toutes les données, on tiendra à ce que chaque catégorie de données soit sur son propre tableau.

Gravité

Probabilité	Faible	Moyenne	Élevée
Faible			
Moyenne			
Élevée			

FIG. 3 : TABLEAU DE CLASSIFICATION DES RISQUES

La gravité est fonction de l'impact du risque sur l'organisme. Cette classification est généralement financière. Définir à partir de quelle perte financière l'impact est perceptible et quel montant n'est pas supportable, revient à la Direction de l'organisme. La gravité est faible pour les sinistres donc les conséquences financières se situent sous le seuil du perceptible, ceux donc le coût n'est pas supportable ont une gravité élevée, les autres sont dans la catégorie moyenne.

L'évaluation de la gravité est difficile pour certains sinistres car, certains coûts sont difficilement déchiffrables, notamment ceux qui touchent à la perte d'image de marque de l'organisation ou au mécontentement de la clientèle.

Pour les risques qui ne sont ni assumés, ni transférés, il sera question de détailler les mesures sélectionnées : dispositifs techniques, procédures, chartes, etc.

Les risques à forte gravité doivent faire l'objet de plusieurs mesures.

- **Mise en œuvre**

La mise en œuvre de la politique de sécurité nécessite de travailler sur la planification des actions mais aussi sur la gestion des changements. Une mise en œuvre d'une politique de sécurité qui ne tient pas compte de la culture d'entreprise, des habitudes et des opinions est vouée à l'échec.

- **Contrôle et révision**

Il ne suffit pas de mettre en place une politique de sécurité, il importe d'en assurer la surveillance et la mise à jour.

Les périodicités de contrôle et les méthodes d'audit doivent être spécifiées dès la conception de la politique de sécurité et faire partie intégrante de la mise en œuvre de la sécurité des systèmes d'information. Une mise en œuvre de tableaux de bord utilisant des données collectées automatiquement est recommandée, de manière à garder en tout temps une vision claire de l'efficacité des mesures et donc du niveau de sécurité fourni par la politique de sécurité.

La révision de la politique de sécurité doit être déclenchée :

- À la suite d'un incident démontrant une erreur de choix en matière de gestion des risques (par exemple, l'incident devait être de faible gravité et a été considéré comme assumé mais le coût a dépassé les prévisions)
- À la suite d'un incident dû à un disfonctionnement de la mesure qui devait l'éviter
- En cas de modification de la stratégie de l'organisme : nouvelles activités, changement de type de clientèle, etc.
- En cas de modification de l'environnement opérationnel de l'organisme: nouvelle procédure, déménagement, télétravail, etc.
- En cas des changements majeurs dans son système d'information : migration vers de nouveau logiciels, nouvelles liaisons réseau, etc.
- En cas de changement des relations avec les partenaires : nouveau contrat d'infogérance, nouveaux fournisseurs
- Lorsque les contraintes légales évoluent.

8.5 Ressources

La mise en place d'un ISMS par un organisme nécessite des ressources financières, humaines, etc. Ces ressources sont le plus souvent le principal handicap d'une mise en place d'un ISMS pour la plupart des organismes. Un organisme doit être à mesure de fournir les garanties nécessaires en ressources pour le bon fonctionnement de son ISMS. Ces ressources tout comme les autres éléments de l'ISMS, doivent être contrôlée et révisée.

8.6 Procédures, guides et chartes (Source : Sécurité de l'information, Élaboration et gestion de la politique de l'entreprise suivant l'ISO 17799, Daniel Linlaud, AFNOR 2003)

Les procédures, guides et chartes constituent la traduction concrète des règles décrites dans les politiques de sécurité de l'information ; dans la catégorie des guides, il est possible de distinguer les « guides d'utilisation » et les « guides d'exploitation ».

8.6.1 Contenu commun aux documents

Les procédures, guides d'utilisation, guides d'exploitation et chartes débutent par les mêmes informations :

- Une référence permettant d'établir un lien entre le document concerné et une règle décrite dans les politiques.
- Un titre concis, permettant d'identifier facilement la portée du document.
- Un cartouche de suivi des différentes versions, comme pour tous les documents constituant le système de gestion de la sécurité de l'information.

8.6.2 Les procédures

Elles décrivent une suite ordonnée d'actions visant à l'atteinte d'un objectif (par exemple : la procédure d'administration des « comptes utilisateurs » décrit les rôles des différents intervenants dans le processus de gestion des droits d'accès logique aux informations) ;

Outre les informations listées au § 8.6.1, une procédure contient, au minimum, les informations suivantes :

- Un résumé destiné à décrire brièvement son contenu ;
- la liste des acteurs intervenants dans la réalisation du processus, qui doit indiquer le titre de chaque intervenant et un bref résumé de son rôle et de ses responsabilités ;
- pour assurer la stabilité des procédures, il ne faut pas nommer les acteurs mais indiquer seulement leurs fonctions ;
- La description ordonnée des tâches, avec indication du point d'entrée (l'événement déclencheur), de l'acteur concerné et le travail à réaliser pour ce dernier.

8.6.3 Guide d'utilisation

Ils sont des recueils de prescription pour un bon usage d'un ou de plusieurs dispositifs du système d'information (par exemple le guide d'utilisation du poste de travail informatique présente un exemple de préceptes destiné aux utilisateurs, en complément éventuel d'une charte abordant des aspects plus juridiques.

Outre les informations listées au § 8.6.1, un guide d'utilisation contient, au minimum, les informations suivantes :

- Liste des principes d'utilisation s'appliquant au dispositif du système d'information, objet du guide d'utilisation ;
- Description détaillée de chaque principe ;

Un guide d'utilisation doit être adapté à la population visée ; par exemple, un guide destiné aux utilisateurs emploiera des termes simples, en évitant un langage trop technique.

8.6.4 Guide d'exploitation

Les guides d'exploitation, qui décrivent de manière détaillée les tâches d'administration, sont destinés aux informaticiens chargés d'un ou de plusieurs dispositifs du système d'information.

Outre les informations listées au § 8.6.1, un guide d'exploitation contient des informations essentiellement techniques, dont la nature exacte dépend du type de dispositif concerné.

Parmi les informations pouvant figurer dans un guide d'exploitation nous avons :

- Liste des contacts utiles (interlocuteurs «sécurité », assistance, maintenance, support, responsable de processus). Les guides d'exploitation sont des documents fortement évolutifs et à usage opérationnel qui, par conséquent, peuvent inclure les coordonnées des acteurs concernés.
- Liste des contrats de maintenance (conditions d'intervention, délais, mode de prise en charge, horaires, etc.).
- Éléments ayant trait à la gestion des accès logiques, notamment en ce qui concerne les comptes privilégiés. Naturellement, ce document ne doit contenir aucun mot de passe.
- Configuration système ; il s'agit d'une description complète de la machine concernée : capacité de traitement, cartes internes, options disponibles, périphériques.
- Caractéristiques du système d'exploitation.
- Description du réseau sur lequel est connecté le dispositif concerné.

- Planification des tâches d'exploitation.
- Procédure d'arrêt de mise en marche du dispositif.
- Procédure de sauvegarde et de restauration des données.
- Gestion des accès logiques.
- Manipulation des données produites : utilisation de papier spécifique, données confidentielles nécessitant une remise à main propre, instruction pour la destruction sécurisée des données de sortie résultant d'une tâche défaillante, etc.
- Suivi du système : détection des erreurs, exploitation, occupation des disques, messages délivrés par le système d'exploitation, etc.
- Journal des problèmes rencontrés et des solutions apportées avec, au minimum, la date et l'heure, la description du problème et de sa solution ainsi que le nom du responsable.
- Journal des incidents de sécurité avec, au minimum, la date et l'heure, la description de l'incident et de la procédure adaptée pour y palier ainsi que le nom du responsable.

8.6.5 Charte orientée utilisateurs

Une charte d'utilisation des ressources du système d'information ou, d'utilisation des ressources informatiques, doit remplir trois objectifs :

- Définir clairement les droits et les devoirs des utilisateurs; il s'agit de la dimension informative de la charte;
- Informer les utilisateurs sur les comportements à risque devant être évités, les sensibiliser aux enjeux de la sécurité de l'information et au rôle très actif qu'ils doivent jouer; il s'agit de la dimension pédagogique de la charte.
- mettre à la disposition de l'organisme les moyens juridiques de se protéger et, si nécessaire, de sanctionner ou de saisir les tribunaux compétents, c'est la dimension juridique de la charte.

Dans le but de favoriser une prise de conscience des enjeux de la sécurité de l'information par les utilisateurs, il est souhaitable que la charte d'utilisation des ressources informatiques ne soit pas simplement une liste d'interdictions de toutes sortes.

La charte d'utilisation des ressources informatiques doit être rédigée dans un langage clair en prenant soin de ne pas utiliser un vocabulaire technique, informatique ou juridique ou, si cela est indispensable, de faire suivre ces termes d'une définition explicite.

8.6.6 Charte orientée fournisseurs

Cette charte constitue une « convention cadre » qui présente les conditions générales d'accès sécurisé aux ressources du système d'information pour des tiers.

La charte de sécurité destinée aux fournisseurs et aux prestataires présentera les critères communs de sécurité ou, en d'autres termes, les contraintes qui s'imposent à tous.

8.7 Sensibilisation et formation des utilisateurs

L'objectif général est de s'assurer que les utilisateurs sont concernés par la sécurité de l'information et conscients des menaces, et qu'ils sont équipés pour appliquer la politique de sécurité de l'organisme dans le cadre de leur travail.

L'organisme doit assurer la formation des utilisateurs à l'utilisation des dispositifs constituant le système d'information et leur sensibilisation aux problèmes de sécurité de l'information.

Ces actions de sensibilisation présenteront les aspects organisationnels, techniques et légaux du dispositif et viendront en complément de la charte d'utilisation des ressources informatiques.

8.8 Installation des dispositifs

L'installation et l'activation des dispositifs de contrôle doivent faire l'objet d'une campagne d'explication pour éviter que les utilisateurs du système d'information ne vivent la mise en place de l'ISMS comme une contrainte restreignant fortement leur liberté individuelle. Tout ceci dépend de l'importance qui sera donnée à la phase de sensibilisation et à la visibilité que pourront avoir les différents acteurs sur des aspects formels comme l'amélioration de la qualité de service, l'augmentation de la rentabilité, l'usage rationnel des indicateurs fournis par les contrôles.

8.9 Procédures d'alerte

Pour assurer une réponse rapide, efficace et ordonnée lorsqu'un incident de sécurité se produit, l'organisme doit définir des procédures et nommer des personnes qui en sont responsables. Les données de journalisation et les preuves doivent être rassemblées et conservées de manière sécurisée.

8.10 audits

L'audit de sécurité est une nécessité dès lors que l'organisme exploite un système d'information. Et cela, quelque soit sa taille et son activité.

L'audit de sécurité a pour objectif de mesurer les éléments critiques de l'organisme, ses processus métier, ses outils de production dont son système informatique, d'identifier les risques qui pèsent sur ces derniers et, enfin, de confronter l'ensemble aux pratiques de sécurité existantes. Cette matrice complexe permet alors de mieux attribuer les ressources de sécurité de l'organisme qui, sont forcément limitées, afin de couvrir les risques les plus pressants ou de protéger les valeurs les plus critiques. Un véritable audit de sécurité sera d'abord organisationnel et ensuite technique.

8.11 Évolution (correction, amélioration, prévention)

Dans cette phase il s'agira de tenir compte de l'évolution permanente des risques en raison de l'influence de paramètres divers tant internes qu'externes à l'organisme. La gestion des incidents (correction) nécessite que soit mise en place une organisation très performante basée sur la responsabilisation des acteurs, sur une excellente réactivité et sur des procédures prévoyant notamment des systèmes d'escalade. La prévention étant un moyen efficace d'améliorer le fonctionnement d l'ISMS, des processus de suivi en temps réel de l'exploitation (le monitoring) seront installés sur les points sensibles du système d'information.

Conclusion

L'information étant l'une des ressources les plus importantes d'un organisme, celui-ci se doit d'assurer sa sécurité. Un organisme qui n'a pas la maîtrise de son système d'information est en danger.

Il est difficile de pouvoir assurer la sécurité des valeurs inconnues, il est donc indispensable de pouvoir et savoir recenser ses biens pour réussir à les protéger. Les systèmes d'information n'échappent pas à cette logique, leur sécurité exige la connaissance de leur valeur, cette valeur qui le plus souvent est fonction de leur importance vis-à-vis des fonctions stratégiques de l'organisme.

Les dangers auxquels s'exposent les organismes à travers leur système d'informations sont si inquiétants que la sécurité de ces derniers doit aujourd'hui faire partie des principaux objectifs de tout organisme.

La mise en place de l'ISMS grâce à la norme ISO 27001 et aux autres basée sur la sécurité des systèmes d'information est, le moyen de permettre à un organisme de mieux connaître son système d'information et de mieux assurer sa protection.

Les PME/PMI trouveront dans ce travail un outil assez intéressant leur permettant de mettre en place un ISMS adapté à leur structure et à leurs fonctions stratégiques.

Bibliographie

Sécurité de l'information, Élaboration et gestion de la politique de l'entreprise suivant l'ISO 17799, Daniel Linlaud, AFNOR 2003.

International Standard ISO/IEC FDIS 177999, 2005-02-11

International Standard ISO/IEC 27001, Première édition 2005-10-15

Management de la SI – Une approche normative. CLUSIF 2004

Internet

http://www.clusis.ch/

http://www.ysosecure.com/enjeux-securite/enjeux-securite-information.asp

http://www.commentcamarche.net/entreprise/e-business.php3

http://www.ssi.gouv.fr/fr/confiance/documents/Methodes/

http://www.hsc.fr/ressources/presentations/

http://iso17799.safemode.org/index.php?page=ISO_17799_and_information_security_awareness

http://iso-17799.safemode.org/index.php?page=Statement_of_Applicability

http://www.afaq.org/web/Espace_clients.nsf?opendatabase&URL=/web/afaqinstit.nsf/volfr/sersom

https://www.clusif.asso.fr/fr/production/ouvrages/